AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR AN ANTICIPATORY SEARCH WARRANT

I, Terrance L. Taylor, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge HSI Charleston, West Virginia. I have experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

2. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, West Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of Inspector General for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center ("FLETC") and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. I have specifically received training in the areas of child pornography and the sexual exploitation

and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2256.

3. As a Special Agent, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the FLETC, Immigration and Customs Enforcement, as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the District of Southern West Virginia. I have received training in the areas of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

4. I make this affidavit in support of an application for an anticipatory search warrant under Federal Rule of Criminal Procedure 41(b)(1), to search for and seize contraband, evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 2251 (production of child pornography) and 2252A (transport, receipt, distribution, possession, and access with intent to

view child pornography) (collectively, the "Subject Offenses"). Specifically, I seek authorization to search for and seize the items more fully set forth in Attachment B of this affidavit.

5. These items are believed to be contained in information associated with the Mega LTD ("Mega") account ultimatew31@gmail.com[1]—respectively, the "Subject Account Information" and the "Subject Account." The Subject Account Information is currently believed to be stored on Mega servers in New Zealand, but is anticipated to be downloaded to computer media in the possession of HSI in the Southern District of West Virginia, as further described in Attachment A.

6. The facts set forth in this affidavit are based upon my investigation, my training and experience, and information I have received from other law enforcement officers and witnesses. Because I am submitting this affidavit for the limited purpose of obtaining a search warrant, I have not included each and every fact I know about this investigation. Instead, I have set forth only the facts that I believe are sufficient to establish probable cause that contraband, evidence, fruits, and/or instrumentalities of violations of the Subject Offenses will be located in the Subject Account Information at the time the warrant is executed.

BACKGROUND ON MEGA

7. In my training, experience, and research, I have learned that Mega is a company that provides file-hosting and communications services to the public, through the website Mega.nz. Mega is headquartered at Level 21, Huawei Centre, 120 Albert Street, Auckland, New Zealand.

[1] As described in paragraph eight, a Mega username takes the form of the full email address submitted by the user to create the account.

On information and belief, Mega's computer servers are located in New Zealand, and Mega does not have offices or employees in the United States.

8. A Mega user can sign up for an account with a valid email address, which becomes the user's Mega username. Mega provides users with a certain amount of free data storage; if a user wants more storage, the user can pay for it. Users can access Mega through the Internet from most major devices and platforms, from anywhere in the world. For example, a user may take a photo with their cell phone, upload that photo to Mega, and then delete the photo from their cell phone. The photo now resides on Mega's servers. The user can then access their Mega account from a different device, such as a desktop computer, and download the photo to that computer.

9. A Mega user can designate a special folder (or folders) on their computer, which Mega synchronizes with the user's account. As a result, that same folder, with the same contents, will appear on both the user's computer and their Mega account. Files placed in that folder are accessible through Mega's website, as well as its mobile-phone applications.

10. In addition, Mega users can share files with other people by sending web links, which give access to the particular shared files.

11. Another feature of Mega is "MegaChat," which allows users to exchange messages and hyperlinks and have audio, video, and group chats.

12. According to Mega, data associated with a Mega account is stored on Mega's servers in an encrypted format. Data is also transmitted in an encrypted format between Mega's servers and users' devices. Messages between Mega users are also transmitted in an encrypted format within Mega's secure server network. Because data is encrypted at all steps, the risk of files or messages being intercepted is minimal.

13. Mega's server architecture means that data is encrypted in a way that makes it generally inaccessible to Mega. Data is encrypted on the client side using an encryption key to which Mega does not have access. This means that, barring exceptional circumstances, Mega does not have the technical ability to decrypt user's files or messages and, as a result, Mega is unable to provide data in a usable format to third parties. Mega also is unable to conduct data recovery. If a user forgets their password, Mega cannot recover that user's data.

14. As explained herein, the Subject Account Information may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This information can indicate who used or controlled the Subject Account. For example, communications, contacts lists, and files sent or uploaded (and the metadata associated with the foregoing, such as date and time) may indicate who used or controlled the Subject Account at a relevant time. The information may also reveal the identity of other victims and the underlying time frames in which they were victimized (e.g., folders with victim data and the metadata associated with file transfers). Additionally, stored electronic data may provide relevant insight into the Subject Account owner's state of mind as it relates to the offenses under investigation. For example, information in the Subject Account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime) or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

PROBABLE CAUSE

15. On or about August 22, 2021, MediaLab/Kik submitted CyberTip Report 98779073 to the NCMEC CyberTipline. The CyberTip Report was the result of MediaLab/Kik representatives reporting to NCMEC that a Kik profile bearing the username "jsparrow2174" had uploaded eight (8) videos and one (1) image through Kik Messenger. Kik representatives viewed the aforementioned files and found them to contain depictions of prepubescent and pubescent minors engaged in sexual activity. Kik representatives advised the aforementioned files were sent from "jsparrow2174."

16. In Cybertip Report 98779073, MediaLab/Kik reported the following information regarding Kik user "jsparrow2174" uploading eight videos and one image of apparent child pornography between on or about July 13, 2021, and on or about July 16, 2021:

Email Address: ultimatew31@gmail.com

Screen/User Name: jsparrow2174

IP Address: 47.220.40.206 on 08-19-2021 at 21:35:46 UTC

NCMEC Geo-Lookup: Elkview, WV, Suddenlink Communications

17. On or about September 16, 2021, HSI Charleston issued an administrative subpoena/summons to Suddenlink Communications regarding subscriber information pertaining to IP address 47.220.40.206 on July 13, 2021, through July 16, 2021. The information provided by Suddenlink indicated that the IP address was assigned to the Elkview, Kanawha County, West Virginia residence owned by Todd Christopher ROATSEY ("ROATSEY").

18. On October 27, 2021, a federal search warrant was obtained to search the Elkview residence belonging to ROATSEY. The search warrant was executed on October 28, 2021. During

the execution of the search warrant, numerous electronic devices were seized. Among the items seized was a Samsung tablet consistent with the device that had uploaded the images in the Kik Cybertip. This tablet was found to have been reset to factory settings or otherwise had its contents removed during the week prior to the execution of the search warrant. However, law enforcement was able to determine from a forensic review of the device that the Kik application had previously been present on the device.

19. Many of the devices seized have been forensically reviewed. The review of one such device, a Samsung Android cell phone seized from ROATSEY at the time of the search, and the microSD card contained therein, (collectively, "the Phone"), revealed evidence of the use of Mega. Law enforcement was able to determine that a Mega account utilized by defendant had the username costanzag558@gmail.com. Evidence on the Phone indicated that this email address had been accessed from the Phone.

20. Mega provided law enforcement with subscriber and other non-content information regarding to the Mega account for costanzag558@gmail.com. This information indicated that the account had been accessed from IP address 47.220.40.206, which is the same IP address identified in the Kik Cybertip and assigned to the residence belonging to ROATSEY. It also indicated that the account was created in October 2019.

21. The review of the Phone revealed that ROATSEY utilized screen-recording programs, such as Snapsaver, to make video recordings of all activity that appeared on the screen during the time when the screen-recording program was active. Such activity included movement between apps, scrolling through or clicking on anything within apps, any alerts or banners that appeared on the screen, and any typing done by the user. Many of these recordings indicated that

the recordings were documenting the screen of ROATSEY's phone, including alerts for text messages from various family members and screens showing previews of his Kanawha County Schools emails.

22. The forensic review of seized devices revealed a substantial number of saved passwords for various accounts. These passwords consisted primarily of two general passwords with slight variations (such as capitalization, numbers, or special characters). The password for the costanzag558@gmail.com Mega account was also specifically identified.

23. The review of the Phone additionally located an approximately four-minute video file (the "Subject Video"), created on or about April 29, 2021, that depicted one such screen-recording of ROATSEY's device. The Subject Video depicted the user opening a folder on the Phone labeled "Productivity." Within this folder was the Mega app. The user opened the Mega app, which displayed numerous folders with names such as "Cp + Rape mixed" and "CP Full." The user accessed several folders and scrolled through dozens of thumbnail previews for videos that could be played by the user (as each video preview had a Play triangle symbol on it). Based solely upon the single frame previewed for each video, the folders contained videos depicting vaginal penetration of toddlers with adult male penises, sado-masochistic bondage of minors, and slight vaginal penetration of what appeared to be an approximately 2- to 3-month-old infant through use of an object.

24. On December 23, 2021, a federal anticipatory search warrant was obtained and executed for the costanzag558@gmail.com account following HSI downloading the information from Mega onto a computer in the Southern District of West Virginia through use of the username and password identified during a review of the Phone. This search revealed that the

costanzag558@gmail.com Mega account appeared to have, at one time, stored files; the account contained a variety of named folders and subfolders. Among the folder names were folders labeled "Jenifer Gorgeous 12y Brazillian (perfeita)" and "BRCP bY pedocp." However, all the folders in the account were found to be empty. The account information obtained also indicated that the last log in to the account was in December 2020.

25. The search of the costanzag558@gmail.com Mega account also revealed a conversation between that account and another user ("Nike G") that took place, in pertinent part, on October 8 and 9, 2019. During this conversation, the costanzag558@gmail.com account sent videos depicting child pornography to Nike G. For example, the costanza558@gmail.com account sent Nike G a video that depicted two nude prepubescent females who were positioned to be laying on top of each other; the video was focused on their vaginal areas and depicted an adult male vaginally penetrating both girls with his penis. The conversation also made clear that they were communicating for the purpose of exchanging child pornography. For example, Nike G sent a message to costanzag558 stating "I only have you as contact for CP." He also specifically asked costanzag558 for videos of girls in the 13 to 15 age range "getting fucked." The two frequently discussed the need to make new contacts on Kik. At one point Nike G tells costanzag558 that Kik might be getting shut down, and costanzag558 responded, "Oh no seriously" and "We need to make contacts in here soon."

26. A further review of the Phone revealed that ROATSEY had received emails from Mega that were addressed to a different email address, ultimatew31@gmail.com (which was also the email address associated with the Kik Cybertip). The first such emails were dated January 18, 2021, and related to confirming the email address for a new account (hereinafter the "Subject

Account") and welcoming the user to Mega. This account appears to have been opened the month after the costanzag558@gmail.com account was last accessed. Another email, dated January 23, 2021, thanked the user of the Subject Account for installing the Mega mobile app. Another email to ultimatew31@gmail.com, dated September 26, 2021, warned that the Subject Account was substantially over the limit permitted for a free account – the user was using 36.29 GB of storage, and the limit was 20 GB. Follow up emails regarding the Subject Account being over its storage limit were sent on October 10, 2021, and October 25, 2021 (three days prior to the execution of the search warrant upon ROATSEY's residence and the seizure of the Phone). According to these dates, the Subject Account was in use at the time the Subject Video was created.

27. The information in the Subject Account is currently believed to be stored on Mega servers located in New Zealand. It is my understanding that the Fourth Amendment's warrant requirement generally does not apply to locations outside the territorial jurisdiction of the United States, *see United States v. Stokes*, 726 F.3d 880, 890-93 (7th Cir. 2013), and that a warrant issued under Federal Rule of Criminal Procedure 41 would not authorize the search of a server located in New Zealand under these circumstances. *See also United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990) (describing a warrant issued by a United States magistrate judge as "a dead letter outside the United States"). Therefore, I seek this warrant out of an abundance of caution, to be certain that an examination of information from the Subject Account (i.e., the Subject Account Information) downloaded to computer media in the possession of HSI in the Southern District of West Virginia will comply with the Fourth Amendment and other applicable laws.

CONDITION REQUIRED PRIOR TO EXECUTION

28. As noted above, the forensic review of devices seized from ROATSEY's residence identified the username and password for the Subject Account. Upon information and belief, the information contained in the Subject Account is believed to be located on Mega servers in New Zealand.

29. HSI plans on accessing the Subject Account using password(s) identified in the forensic review of ROATSEY's devices; if such access is successful, HSI intends to use Mega's data transfer tools to download the account's information—again, onto computer media in the possession of HSI, located in the Southern District of West Virginia**.** The downloaded information (i.e., the Subject Account Information) may include, but is not limited to, files, communications, and contact lists associated with the Subject Account.

30. I am seeking permission to search the Subject Account Information following the triggering event of the download of said information by HSI into the Southern District of West Virginia, as described in Attachment A, and to seize the items and information described in Attachment B.

31. *Manner of Execution*. Because this warrant seeks permission only to examine information on computer media in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. Based on the information described above, I respectfully submit there is probable cause to believe that contraband, evidence, fruits, and/or instrumentalities of violations of the

Subject Offenses, specifically those items more fully set forth in Attachment B, are currently located in the Subject Account, and will be located in the Subject Account Information in the Southern District of West Virginia at the time the warrant is executed.

Terrance L. Taylor
Special Agent
Department of Homeland Security
Homeland Security Investigations

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this 28th day of December, 2021.

Omar J. Aboulhosn
United States Magistrate Judge